REMARKS

In the Official Action mailed 23 August 2007, the Examiner reviewed claims 1-4, 6-11, 13-18 and 20-30. The Examiner has rejected claims 23, 24, 26, 27, 29 and 30 under 35 U.S.C. §112, second paragraph; and has rejected claims 1-4, 6-11, 13-18 and 20-30 under 35 U.S.C. §103(a).

Applicant cancels independent claims 1, 8 and 15, and adds new claims 31-39, including independent claims 31, 34 and 37 to replace canceled independent claims 1, 8, and 15. Amendments to all the pending dependent claims except 3, 10 and 17, are made as a consequence of the new independent claims. Also, applicant cancels claims 22-30. Claims 2-4, 6, 7, 9-11, 13, 14, 16-18, 20-21 and 31-39 are now pending.

The rejections are respectfully traversed below and reconsideration is requested.

Rejection of Claims 23, 24, 26, 27, 29 and 30 under 35 U.S.C. §112, second paragraph

The Examiner has rejected claims 23, 24, 26, 27, 29 and 30 under 35 U.S.C. §112, second paragraph. Such claims are canceled.

Rejection of Claims 1-4, 6-11, 13-18 and 20-30 under 35 U.S.C. §103(a)

The Examiner has rejected claims 1-4, 6-11, 13-18 and 20-30 under 35 U.S.C. §103(a) as being unpatentable over Perlman (US 6,363,480), and further in view of Kelly (US 5,636,280).

As mentioned above, independent claims 1, 8 and 15 have been replaced by claims 31, 34 and 37 respectively. Applicant requests reconsideration in view of the remarks submitted 23 October 2007, which are incorporated by reference herein. In addition, substantial clarifying amendments have been entered.

Support for New Claims 31-39

Support in the specification for new claims 31-39 is found in Figures 1, 2, and 3, and in the specification. Copies of such claims with parenthetical references to support in the specification follow:

31. (new) A method for mutual authentication in communications between first and second stations, comprising:

generating and storing a set of ephemeral session keys at the first station, ephemeral session keys in the set being associated with respective session key initiation intervals, and being discarded at a time later than expiration of the respective session key initiation intervals; (SRKs, Fig. 1)

in response to a request (3005, Fig. 3) to initiate a communication session received by the first station during a particular session key initiation interval, selecting the associated session key (SRKi, Fig. 3);

sending a message carrying said associated session key to the second station (3006, Fig. 3), and receiving a response from the second station including a digital identifier (host ID or user name), ~~which is~~ the digital identifier being information shared between the first station and the second station, or between the first station and a user at the second station, the digital identifier being encrypted using said associated session key to verify receipt of the session key by the second station and to identify the second station or the user of the second station (3007, 3008, Fig. 3);

generating and storing, in the first station, a set of intermediate data keys, the set of intermediate data keys including intermediate data key (i), for i = 1 to at least n, and being discarded at a time later than expiration of the particular session key initiation interval; (DRK1 to DRKn, Fig. 2)

executing a first set of exchanges (3009-3013, Fig. 3) including one or more exchanges with the second station, after verifying in said first station receipt of the session key by the second station by decrypting the digital identifier using the associated session key at the first station and positively matching the decrypted digital identifier against an existing entry in a stored list of authorized users, the first set of exchanges including

sending a message to the second station carrying intermediate data key (i) from said set of intermediate data keys encrypted using the associated session key for a first exchange in first set of exchanges and using the intermediate data key (i-1) for subsequent exchanges in the first set of exchanges,

receiving a response from the second station including a hashed version of intermediate data key (i) encrypted using intermediate data key (i), ~~and~~ decrypting the hashed version of the intermediate data key (i), calculating a hashed version of intermediate data key (i) at the first station, and matching the calculated hashed version and the received hashed version of intermediate data key (i) to verify receipt by the second station of intermediate data key (i);

executing a second set of exchanges for mutual authentication after verifying in said first station receipt of the intermediate data key (n-1) by the second station, including

sending a first message carrying intermediate data key (n) encrypted using a hashed version of a first shared secret,

receiving a response from the second station carrying a hashed version of intermediate data key (n) encrypted using a hashed version of the first shared secret, and decrypting the hashed version of the intermediate data key (n) , calculating a hashed version of intermediate data key (n) at the first station, and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) to verify possession by the second station of the first shared secret (3014, Fig. 3);

sending a second message carrying intermediate data key (n) encrypted using a hashed version of a second shared secret; and

if the second station sends a response to the second message, carrying a hashed version of intermediate data key (n) encrypted using a hashed version of the second shared secret, after possession by the first station of the second shared secret is verified at the second station, the verifying being accomplished at the second station by decrypting the intermediate data key (n) from the second message using the hashed version of the second shared secret, calculating a hashed version of the intermediate data key (n), and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) to verify possession by the first station of the second shared secret (3015, Fig. 3), then

receiving the response from the second station, and decrypting the hashed version of the intermediate data key (n) using the hashed version of the second shared secret, calculating a hashed version of intermediate data key (n) at the first station, and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) at the first station to verify mutual authentication of the first and second stations (3015, Fig. 3); and if mutual authentication is verified at the first station, then sending a message indicating successful authentication (3016, Fig. 3).

32. (new) The method of claim 31, wherein said message indicating successful authentication carries a signal encrypted using intermediate data key (n-1) or using another prearranged one of said intermediate data keys (i) (3016, Fig. 3).

33. (new) The method of claim 31, including using intermediate data key (n) as a symmetrical key to encrypt data during post-authentication ~~in~~ communications between the first and second stations in the communication session (FSK, paragraph [0051]).

34.(new) A data processing apparatus, comprising:

a processor associated with a first station, a communication interface adapted for connection to a communication medium, and memory storing instructions for execution by the data processor, the instructions including

logic to receive a request via the communication interface for initiation of a communication session between a first station and a second station;

logic to provide for mutual authentication in communications between the first station and a second station, comprising:

generating and storing a set of ephemeral session keys at the first station, ephemeral session keys in the set being associated with respective session key initiation intervals, and being discarded at a time later than expiration of the respective session key initiation intervals; (SRKs, Fig. 1)

in response to a request (3005, Fig. 3) to initiate a communication session received by the first station during a particular session key initiation interval, selecting the associated session key (SRKi, Fig. 3);

sending a message carrying said associated session key to the second station (3006, Fig. 3), and receiving a response from the second station including a digital identifier (host ID or user name), ~~which is~~ the digital identifier being information shared between the first station and the second station, or between the first station and a user at the second station, the digital identifier being encrypted using said associated session key to verify receipt of the session key by the second station and to identify the second station or the user of the second station (3007, 3008, Fig. 3);

generating and storing, in the first station, a set of intermediate data keys, the set of intermediate data keys including intermediate data key (i), for i = 1 to at least n, and being discarded at a time later than expiration of the particular session key initiation interval; (DRK1 to DRKn, Fig. 2)

executing a first set of exchanges (3009-3013, Fig. 3) including one or more exchanges with the second station, after verifying in said first station receipt of the session key by the second station by decrypting the digital identifier using the associated session key at the first station and positively matching the decrypted digital identifier against an existing entry in a stored list of authorized users, the first set of exchanges including

sending a message to the second station carrying intermediate data key (i) from said set of intermediate data keys encrypted using the associated session key for a first exchange in first set of exchanges and using the intermediate data key (i-1) for subsequent exchanges in the first set of exchanges,

receiving a response from the second station including a hashed version of intermediate data key (i) encrypted using intermediate data key (i), ~~and~~ decrypting the hashed version of the intermediate data key (i), calculating a hashed version of intermediate data key (i) at the first station, and matching the calculated hashed version and the received hashed version of intermediate data key (i) to verify receipt by the second station of intermediate data key (i);

executing a second set of exchanges for mutual authentication after verifying in said first station receipt of the intermediate data key (n-1) by the second station, including

sending a first message carrying intermediate data key (n) encrypted using a hashed version of a first shared secret,

receiving a response from the second station carrying a hashed version of intermediate data key (n) encrypted using a hashed version of the first shared secret, and decrypting the hashed version of the intermediate data key (n) , calculating a hashed version of intermediate data key (n) at the first station, and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) to verify possession by the second station of the first shared secret (3014, Fig. 3);

sending a second message carrying intermediate data key (n) encrypted using a hashed version of a second shared secret; and

if the second station sends a response to the second message, carrying a hashed version of intermediate data key (n) encrypted using a hashed version of the second shared secret, after possession by the first station of the second shared secret is verified at the second station, the verifying being accomplished at the second station by decrypting the intermediate data key (n) from the second message using the hashed version of the second shared secret, calculating a hashed version of the intermediate data key (n), and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) to verify possession by the first station of the second shared secret (3015, Fig. 3), then

receiving the response from the second station, and decrypting the hashed version of the intermediate data key (n) using the hashed version of the second shared secret, calculating a hashed version of intermediate data key (n) at the first station, and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) at the first station to verify mutual authentication of the first and second stations (3015, Fig. 3); and

if mutual authentication is verified at the first station, then sending a message indicating successful authentication (3016, Fig. 3).

35. (new) The apparatus of claim 34, wherein said message indicating successful authentication carries a signal encrypted using intermediate data key (n-1) or using another prearranged one of said intermediate data keys (i) (3016, Fig. 3).

36. (new) The apparatus of claim 34, including using intermediate data key (n) as a symmetrical key to encrypt data during post-authentication communications between the first and second stations in the communication session (FSK, paragraph [0051]).

37. (new) An article, comprising:

machine readable data storage medium having computer program instructions stored therein for establishing a communication session on a communication medium between a first data processing station and a second data processing station having access to the communication medium, said instructions comprising

logic to receive a request via the communication interface for initiation of a communication session between a first station and a second station;

logic to provide for mutual authentication in communications between the first station and a second station, comprising:

generating and storing a set of ephemeral session keys at the first station, ephemeral session keys in the set being associated with respective session key initiation intervals, and being discarded at a time later than expiration of the respective session key initiation intervals; (SRKs, Fig. 1)

in response to a request (3005, Fig. 3) to initiate a communication session received by the first station during a particular session key initiation interval, selecting the associated session key (SRKi, Fig. 3);

sending a message carrying said associated session key to the second station (3006, Fig. 3), and receiving a response from the second station including a digital identifier (host ID or user name), ~~which is~~ the digital identifier being information shared between the first station and the second station, or between the first station and a user at the second station, the digital identifier being encrypted using said associated session key to verify receipt of the session key by the second station and to identify the second station or the user of the second station (3007, 3008, Fig. 3);

generating and storing, in the first station, a set of intermediate data keys, the set of intermediate data keys including intermediate data key (i), for i = 1 to at least n, and being discarded at a time later than expiration of the particular session key initiation interval; (DRK1 to DRKn, Fig. 2)

executing a first set of exchanges (3009-3013, Fig. 3) including one or more exchanges with the second station, after verifying in said first station receipt of the session key by the second station by decrypting the digital identifier using the associated session key at the first station and positively matching the decrypted digital identifier against an existing entry in a stored list of authorized users, the first set of exchanges including

sending a message to the second station carrying intermediate data key (i) from said set of intermediate data keys encrypted using the associated session key for a first exchange in first set of exchanges and using the intermediate data key (i-1) for subsequent exchanges in the first set of exchanges,

receiving a response from the second station including a hashed version of intermediate data key (i) encrypted using intermediate data key (i), ~~and~~ decrypting the hashed version of the intermediate data key (i), calculating a hashed version of intermediate data key (i) at the first station, and matching the calculated hashed version and the received hashed version of intermediate data key (i) to verify receipt by the second station of intermediate data key (i);

executing a second set of exchanges for mutual authentication after verifying in said first station receipt of the intermediate data key (n-1) by the second station, including

sending a first message carrying intermediate data key (n) encrypted using a hashed version of a first shared secret,

receiving a response from the second station carrying a hashed version of intermediate data key (n) encrypted using a hashed version of the first shared secret, and decrypting the hashed version of the intermediate data key (n) , calculating a hashed version of intermediate data key (n) at the first station, and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) to verify possession by the second station of the first shared secret (3014, Fig. 3);

sending a second message carrying intermediate data key (n) encrypted using a hashed version of a second shared secret; and

if the second station sends a response to the second message, carrying a hashed version of intermediate data key (n) encrypted using a hashed version of the second shared secret, after possession by the first station of the second shared secret is verified at the second station, the verifying being accomplished at the second station by decrypting the intermediate data key (n) from the second message using the hashed version of the second shared secret, calculating a hashed version of the intermediate data key (n), and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) to verify possession by the first station of the second shared secret (3015, Fig. 3), then

receiving the response from the second station, and decrypting the hashed version of the intermediate data key (n) using the hashed version of the second shared secret, calculating a hashed version of intermediate data key (n) at the first station, and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) at the first station to verify mutual authentication of the first and second stations (3015, Fig. 3); and

if mutual authentication is verified at the first station, then sending a message indicating successful authentication (3016, Fig. 3).

38. (new) The apparatus of claim 37, wherein said message indicating successful authentication carries a signal encrypted using intermediate data key (n-1) or using another prearranged one of said intermediate data keys (i) (3016, Fig. 3).

39. (new) The apparatus of claim 37, including using intermediate data key (n) as a symmetrical key to encrypt data during post-authentication communications between the first and second stations in the communication session (FSK, paragraph [0051]).

///

CONCLUSION

It is respectfully submitted that this application is now in condition for allowance, and such action is requested.

The Commissioner is hereby authorized to charge any fee determined to be due in connection with this communication, or credit any overpayment, to our Deposit Account No. 50-0869 (AIDT 1005-1).

Respectfully submitted,

Dated: 11 February 2008

/Mark A. Haynes/
Mark A. Haynes, Reg. No. 30,846

HAYNES BEFFEL & WOLFELD LLP
P.O. Box 366
Half Moon Bay, CA 94019
(650) 712-0340 phone
(650) 712-0263 fax